

AMENDMENTS TO THE CLAIMS

1 1. (currently amended) A method of controlling access of network management requests
2 directed to one or more network devices that participate in a virtual private network,
3 the method comprising the computer-implemented steps of:
4 receiving a request, from a first network device participating in a virtual private
5 network, to carry out a management protocol operation that involves one or
6 more managed objects associated with one or more second network devices
7 participating in the virtual private network;
8 determining an identifier of [[a]] the virtual private network in the request to carry out
9 the management protocol operation;
10 identifying, among a plurality of managed objects, a subset of objects that requests
11 associated with the virtual private network are permitted to access; and
12 in response to the request, providing the request with to the first network device
13 access to only the subset of objects.

1 2. (original) A method as recited in Claim 1, further comprising the steps of providing,
2 at one of the network devices, a mapping of a plurality of identifiers of virtual private
3 networks to corresponding views of subsets of managed objects.

1 3. (previously presented) A method as recited in Claim 1, further comprising the steps of
2 providing, at one of the network devices, a mapping of a plurality of identifiers of
3 virtual private networks to corresponding views of subsets of managed objects, in the
4 form of one or more entries in a view-based access control model table that associate

SNMPv3 securityName values to corresponding MIB (Management Information Base) Views.

4. (previously presented) A method as recited in Claim 1, further comprising the steps of providing, at one of the network devices, one or more entries in a view-based access control model table that associate SNMPv3 securityName values to corresponding MIB (Management Information Base) Views, wherein each of the securityName values is associated with a virtual private network, and wherein the corresponding MIB Views represent access control policies applicable to the associated virtual private networks.

5. (original) A method as recited in Claim 1, further comprising the steps of providing, at one of the network devices, a mapping of a plurality of identifiers of virtual private networks to corresponding views of subsets of managed objects, and wherein the steps of identifying a subset of objects and providing the request with access comprise the steps of:
determining whether the identifier from the request is in the mapping;
when the identifier from the request is in the mapping:

identifying a management information base variable referenced in the request;
based on one or more views referenced in the mapping, determining whether a protocol operation of the request is allowed for the variable;
dispatching information identifying the variable and the protocol operation to a code implementation of the protocol operation only when the protocol operation is allowed for the variable.

1 6. (previously presented) A method as recited in Claim 1, further comprising the steps of
2 providing, at one of the network devices, a mapping of a plurality of identifiers of
3 virtual private networks to corresponding views of subsets of managed objects, in the
4 form of one or more entries in a view-based access control model table that associate
5 security name values to corresponding MIB (Management Information Base) Views,
6 and wherein the steps of identifying a subset of objects and providing the request with
7 access comprise the steps of:
8 determining whether the identifier from the request is in the view-based access
9 control model table;
10 when the identifier from the request is in the view-based access control model table:
11 identifying a management information base variable referenced in the request;
12 based on one or more MIB Views referenced in the view-based access control
13 model table, determining whether a protocol operation of the request is
14 allowed for the variable;
15 dispatching information identifying the variable and the protocol operation to
16 a code implementation of the protocol operation only when the
17 protocol operation is allowed for the variable.

1 7. (previously presented) A method as recited in Claim 1, further comprising the steps of
2 providing, at one of the network devices, one or more entries in a view-based access
3 control model table that associate SNMPv3 securityName values to corresponding
4 MIB (Management Information Base) Views, wherein each of the securityName
5 values is associated with a virtual private network, and wherein the corresponding

6 MIB Views represent access control policies applicable to the associated virtual
7 private networks, and wherein the steps of identifying a subset of objects and
8 providing the request with access comprise the steps of:
9 determining whether the identifier from the request is in the view-based access
10 control model table;
11 when the identifier from the request is in the view-based access control model table:
12 identifying a management information base variable referenced in the request;
13 based on one or more MIB Views referenced in the view-based access control
14 model table, determining whether a protocol operation of the request is
15 allowed for the variable;
16 dispatching information identifying the variable and the protocol operation to
17 a code implementation of the protocol operation only when the
18 protocol operation is allowed for the variable.

- 1 8. (original) A method as recited in Claim 1, further comprising the steps of:
2 providing, at a network management station that is communicatively coupled to the
3 network devices, a mapping of a plurality of virtual private network identifiers
4 to SNMPv3 securityNames;
5 providing, at the network management station, an executable process that associates a
6 virtual private network identifier with each SNMP request that is issued by the
7 network management station to the network devices.

1 9. (currently amended) A method of controlling access of network management requests
2 directed to one or more network devices that participate in a virtual private network,
3 the method comprising the computer-implemented steps of:
4 receiving, from a network device participating in a virtual private network, a request
5 to carry out a management protocol operation, wherein the request contains an
6 identifier of the virtual private network identifier in a security name value;
7 extracting the security name value, which identifies the virtual private network, and
8 determining a protocol operation that is embodied in the request;
9 using a view-based access control model, matching the security name value, which
10 identifies the virtual private network, to a management information base view
11 that corresponds to the requested operation;
12 processing the requested operation only if access is allowed to managed objects, in
13 the management information base, that are associated with one or more
14 network devices participating in the virtual private network, based on the
15 ~~matching~~ management information base view matching the security name
16 value that identifies the virtual private network.

1 10. (original) A method as recited in Claim 9, further comprising the steps of:
2 determining whether the request can be satisfied;
3 extracting the security name value from a context string in the request.

1 11. (original) A method as recited in Claim 10, wherein the matching step further
2 comprises the steps of:

3 determining whether the security name is in a view-based access control model table;
4 rejecting and returning the request when the security name is not found in the view-
5 based access control model table.

1 12. (original) A method as recited in Claim 10, further comprising the steps of:

2 determining whether the security name is in a view-based access control model table;
3 when the security name is found in the view-based access control model table:

4 identifying a management information base variable referenced in the request;
5 based on one or more views referenced in the view-based access control
6 model table, determining whether the protocol operation is allowed for
7 the variable;

8 dispatching information identifying the variable and the protocol operation to
9 a code implementation of the protocol operation only when the
10 protocol operation is allowed for the variable.

1 13. (previously presented) The method as recited in Claim 10, further comprising the
2 steps of:

3 determining whether the security name is in a view-based access control model table;
4 when the security name is found in the view-based access control model table:

5 identifying a management information base variable referenced in the request;
6 based on one or more views referenced in the view-based access control
7 model table, determining whether the protocol operation is allowed for
8 the variable;

9 dispatching information identifying the variable and the protocol operation to
10 a code implementation of the protocol operation only when the
11 protocol operation is allowed for the variable;
12 determining whether a virtual private network identifier is referenced in the
13 request, processing the request using managed information objects in a
14 default view when no virtual private network identifier is referenced in
15 the request, and processing the request using management information
16 objects in a view corresponding to the virtual private network
17 identifier only when a virtual private network identifier is referenced
18 in the request.

1 14. (currently amended) A computer-readable medium carrying one or more sequences of
2 instructions for controlling access of network management requests directed to one or
3 more network devices that participate in a virtual private network, which instructions,
4 when executed by one or more processors, cause the one or more processors to carry
5 out the steps of:

6 receiving a request, from a first network device participating in a virtual private
7 network, to carry out a management protocol operation that involves one or
8 more managed objects associated with one or more second network devices
9 participating in the virtual private network;
10 determining an identifier of [[a]] the virtual private network in the request to carry out
11 the management protocol operation;

12 identifying, among a plurality of managed objects, a subset of objects that requests
13 associated with the virtual private network are permitted to access; and
14 in response to the request, providing the request with to the first network device
15 access to only the subset of objects.

1 15. (original) A computer-readable medium as recited in Claim 14, further comprising
2 instructions which, when executed by the one or more processors, cause the one or
3 more processors to carry out the steps of providing, at one of the network devices, a
4 mapping of a plurality of identifiers of virtual private networks to corresponding
5 views of subsets of managed objects.

1 16. (previously presented) A computer-readable medium as recited in Claim 14, further
2 comprising instructions which, when executed by the one or more processors, cause
3 the one or more processors to carry out the steps of providing, at one of the network
4 devices, a mapping of a plurality of identifiers of virtual private networks to
5 corresponding views of subsets of managed objects, in the form of one or more
6 entries in a view-based access control model table that associate SNMPv3
7 securityName values to corresponding MIB (Management Information Base) Views.

1 17. (previously presented) A computer-readable medium as recited in Claim 14, further
2 comprising instructions which, when executed by the one or more processors, cause
3 the one or more processors to carry out the steps of providing, at one of the network
4 devices, one or more entries in a view-based access control model table that associate
5 SNMPv3 securityName values to corresponding MIB (Management Information
6 Base) Views, wherein each of the securityName values is associated with a virtual

7 private network, and wherein the corresponding MIB Views represent access control
8 policies applicable to the associated virtual private networks.

1 18. (original) A computer-readable medium as recited in Claim 14, further comprising
2 instructions which, when executed by the one or more processors, cause the one or
3 more processors to carry out the steps of providing, at one of the network devices, a
4 mapping of a plurality of identifiers of virtual private networks to corresponding
5 views of subsets of managed objects, and wherein the steps of identifying a subset of
6 objects and providing the request with access comprise the steps of.
7 determining whether the identifier from the request is in the mapping;
8 when the identifier from the request is in the mapping:

9 identifying a management information base variable referenced in the request;
10 based on one or more views referenced in the mapping, determining whether a
11 protocol operation of the request is allowed for the variable;
12 dispatching information identifying the variable and the protocol operation to
13 a code implementation of the protocol operation only when the
14 protocol operation is allowed for the variable.

1 19. (currently amended) An apparatus for controlling access of network management
2 requests directed to one or more network devices that participate in a virtual private
3 network, comprising:
4 means for receiving a request, from a first network device participating in a virtual
5 private network, to carry out a management protocol operation that involves

6 one or more managed objects associated with one or more second network

7 devices participating in the virtual private network;

8 means for determining an identifier of ~~[[a]]~~ the virtual private network in the request

9 to carry out the management protocol operation;

10 means for identifying, among a plurality of managed objects, a subset of objects that

11 requests associated with the virtual private network are permitted to access;

12 and

13 means for providing ~~the request with~~ to the first network device access to only the

14 subset of objects.

1 20. (currently amended) An apparatus controlling access of network management

2 requests directed to one or more network devices that participate in a virtual

3 private network, comprising:

4 a network interface that is coupled to the data network for receiving one or more

5 packet flows therefrom;

6 a processor;

7 one or more stored sequences of instructions which, when executed by the

8 processor, cause the processor to carry out the steps of:

9 receiving a request, from a first network device participating in a virtual

10 private network, to carry out a management protocol operation that

11 involves one or more managed objects associated with one or more

12 second network devices participating in the virtual private

13 network;

determining an identifier of ~~[[a]]~~ the virtual private network in the request
to carry out the management protocol operation;
identifying, among a plurality of managed objects, a subset of objects that
requests associated with the virtual private network are permitted
to access; and
in response to the request, providing the request with to the first network
device access to only the subset of objects.

21. (previously presented) A method of controlling access of network management
requests directed to one or more network devices that participate in one or more
virtual private networks, the method comprising the computer-implemented steps
of:
receiving a request to carry out a SNMP (Simple Network Management Protocol)
operation directed to one or more managed objects from a MIB
(Management Information Base) associated with one or more network
devices that participate in multiple virtual private networks;
determining, from the request, an identifier of a particular virtual private network
of the multiple virtual private networks;
identifying, among a plurality of managed objects from a MIB associated with a
network device from the one or more network devices that participate in
the multiple virtual private networks, a subset of managed objects that
requests associated with the particular virtual private network are
permitted to access; and
in response to the request, providing access to only the subset of managed objects.